

WHAT IS CLAIMED IS:

1. A ring signature creating apparatus, comprising:  
signature-data inputting means for inputting ring  
signature data that can be created with N public keys and a  
private key corresponding to one of the N public keys, that  
allows for signature verification for each of the N public  
keys, and that allows which one of N members has signed to  
be kept secret; and

denial-data generating means for generating denial data  
in accordance with the ring signature data, the denial data  
allowing for verification that a user other than a creator  
of the ring signature data has not signed.

2. A ring signature creating apparatus in a digital  
signature system in which, when a message is digitally  
signed, pre-computed data is compressed together with the  
message with a hash function, the apparatus comprising:

hash computing means for generating first pre-computed  
data and computing an i-th hash value for data that has N  
public keys and at least one private key corresponding to  
the N public keys and that includes the message and an i-th  
pre-computed data;

pseudo computing means for computing the i-th pre-  
computed data and an i-th signature data such that the i-th

hash value appears to have been signed; and  
signing means for generating first signature data  
corresponding to the first pre-computed data from the  
private key, with respect to an N-th hash value obtained  
through sequential computing by the pseudo computing means.

3. The ring signature creating apparatus according to  
claim 2, wherein a digital signature system in which a  
message is digitally signed after only the message is  
compressed with a hash function is changed to the digital  
signature system in which the pre-computed data is  
compressed together with the message with the hash function.

4. The ring signature creating apparatus according to  
claim 2, further comprising means for creating denial data  
for the generated ring signature data, the denial data  
allowing for verification that a user other than a creator  
of the ring signature data has not signed.

5. The ring signature creating apparatus according to  
claim 4, further comprising:

message receiving means for receiving a message to be  
signed;  
ring-signature data receiving means for receiving the  
ring signature data in which a ring signature is attached to

the message;

pledge-data attaching means for attaching pledge data to the message;

accompanying-data extracting means for extracting data needed to re-compute a signature from the ring signature data;

re-signing means for re-signing the pledge-data-attached message created by the pledge-data attaching means; and

denial-data outputting means for outputting data computed by the re-signing means.

6. The ring signature creating apparatus according to claim 5, wherein the re-signing means comprises hash re-computing means for re-computing a hash value for data obtained by the pledge-data attaching means and computational-operation means for performing a computational operation on the hash value computed by the hash re-computing means.

7. The ring signature creating apparatus according to claim 5, wherein the pledge data is replaced with pre-computed data.

8. The ring signature creating apparatus according to

claim 2, wherein the first pre-computed data is a result of computation in which, with respect to a generator g of a multiplicative group of order P-1, pseudo random number k is generated and a computational operation  $g^k \pmod{P}$  is performed, where P is a prime number and  $k < P-1$ .

9. The ring signature creating apparatus according to claim 1, wherein security is based on a discrete logarithm problem.

10. The ring signature creating apparatus according to claim 1, wherein the denial data is proven by interactive communication.

11. A ring signature verifying apparatus in a digital signature system in which, when a message is digitally signed, pre-computed data is compressed together with the message with a hash function, the apparatus comprising:

hash computing means for computing an i-th hash value for data that has N public keys and that includes the message and an i-th pre-computed data;

verification computational-operation means for performing a computational operation for verification of an i-th signature data; and

verifying means for verifying whether an N-th hash

value matches a first hash value, the N-th hash value being obtained through sequential computation by the verification computational-operation means.

12. The ring signature verifying apparatus according to claim 11, wherein a digital signature system in which, when a message is digitally signed, a computational operation is performed after only the message is compressed with a hash function, is changed to the digital signature system in which the pre-computed data is compressed together with the message with the hash function, and the changed digital signature system is executed.

13. The ring signature verifying apparatus according to claim 11 or 12, further comprising means for generating denial data for the ring signature data generated by the ring signature creating apparatus according to claim 1, the denial data allowing for verification that a user other than a creator of the ring signature data has not signed.

14. The ring signature verifying apparatus according to claim 13, further comprising:

signature-message receiving means for receiving a message to be signed;

ring-signature data receiving means for receiving ring

signature data in which a ring signature is attached to the message;

denial-data receiving means for receiving denial data for the ring signature data receiving means;

pledge-data receiving means for receiving pledge data corresponding to the denial data;

accompanying-data extracting means for extracting data needed for verification from the ring signature data;

hash computational-operation means for computing a hash value from the message and the pledge data; and

denial-data verifying means for performing a computational operation on the denial data using the public key to thereby verify whether the resulting denial data matches data obtained by the hash computational-operation means.

15. The ring signature verifying apparatus according to claim 11, wherein security is based on a discrete logarithm problem.

16. The ring signature verifying apparatus according to claim 11, wherein the denial data is proven by interactive communication.

17. A ring signature system, comprising:

the ring signature creating apparatus according to  
claim 1; and

the ring signature verifying apparatus according to  
claim 11.

18. A ring signature creating method, comprising:  
an inputting step of inputting ring signature data that  
can be created with N public keys and a private key  
corresponding to one of the N public keys, that allows for  
signature verification for each of the N public keys, and  
that allows which one of N members has signed to be kept  
secret; and

a denial data generating step of generating denial data  
in accordance with the ring signature data, the denial data  
allowing for verification that a user other than a creator  
of the ring signature data has not signed.

19. A ring signature creating method in a digital  
signature system in which, when a message is digitally  
signed, pre-computed data is compressed together with the  
message with a hash function, the method comprising:

a hash computing step of generating first pre-computed  
data and computing an i-th hash value for data that has N  
public keys and at least one private key corresponding to  
the N public keys and that includes the message and an i-th

pre-computed data;

a pseudo computing step of computing the i-th pre-computed data and an i-th signature data such that the i-th hash value appears to have been signed; and

a signing step of generating first signature data corresponding to the first pre-computed data from the private key, with respect to an N-th hash value obtained through sequential computing in the pseudo computing step.

20. A ring signature verifying method in a digital signature system in which, when a message is digitally signed, pre-computed data is compressed together with the message with a hash function, comprising:

a hash computing step of computing an i-th hash value for data that has N public keys and that includes the message and an i-th pre-computed data;

a verification computational-operation step of performing a computational operation for verification of an i-th signature data; and

a verifying step of verifying whether an N-th hash value matches a first hash value, the N-th hash value being obtained through sequential computation in the verification computational-operation step.

21. A program for causing a computer to realize the

ring signature creating method according to claim 18.

22. A program for causing a computer to realize the  
ring signature creating method according to claim 19.

23. A program for causing a computer to realize the  
ring signature verifying method according to claim 20.